The Overall Classification of this Briefing is
UNCLASSIFIED – CLEARED FOR PUBLIC RELEASE

Odin Program: Presentation Attack Detection

Lars Ericson | Program Manager | November 28, 2018

Office of the Director of National Intelligence

IARPA

BE THE FUTURE

Office of the Director of National Intelligence

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA

Central Intelligence Agency

Defense Intelligence Agency

Department of State

National Security Agency

Department of Energy

National Geospatial-Intelligence Agency

Department of the Treasury

National Reconnaissance Office

Drug Enforcement Administration

Department of the Army

Federal Bureau of Investigation

Department of the Navy

Department of Homeland Security

Air Force

Coast Guard

Marine Corps

IARPA Mission and Method

IARPA's mission is to invest in high-risk/high-payoff research to provide the U.S. with an overwhelming intelligence advantage

- **Bring the best minds to bear on our problems**
  - Full and open competition to the greatest possible extent
  - World-class, rotational Program Managers
- **Define and execute research programs that:**
  - Have goals that are clear, measureable, ambitious and credible
  - Employ independent and rigorous Test & Evaluation (T&E)
  - Involve IC partners from start to finish
  - Run from three to five years
  - Publish peer-reviewed results and data, to the greatest possible extent

Odin Program Goal

Goal: Develop biometric presentation attack detection technologies to detect when someone is attempting to disguise their biometric identity

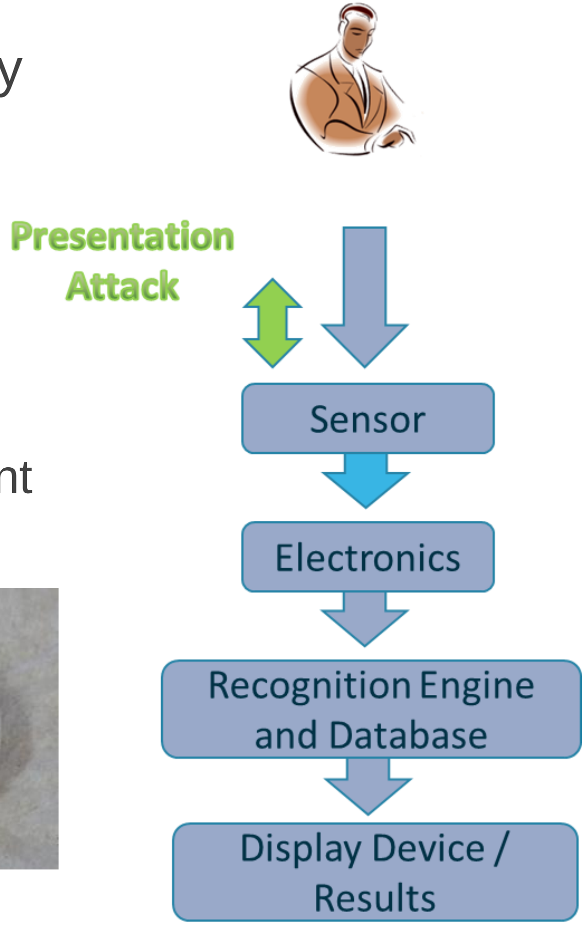
ODIN

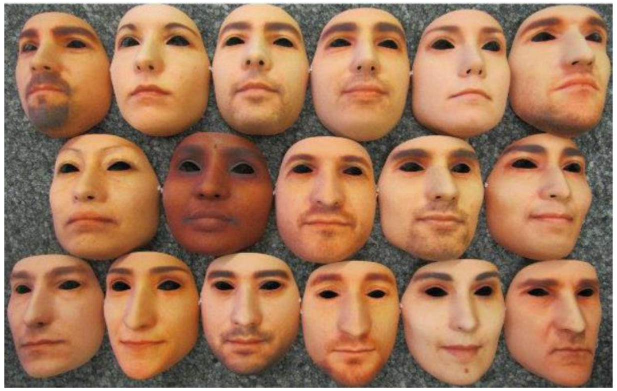
Program Pillars

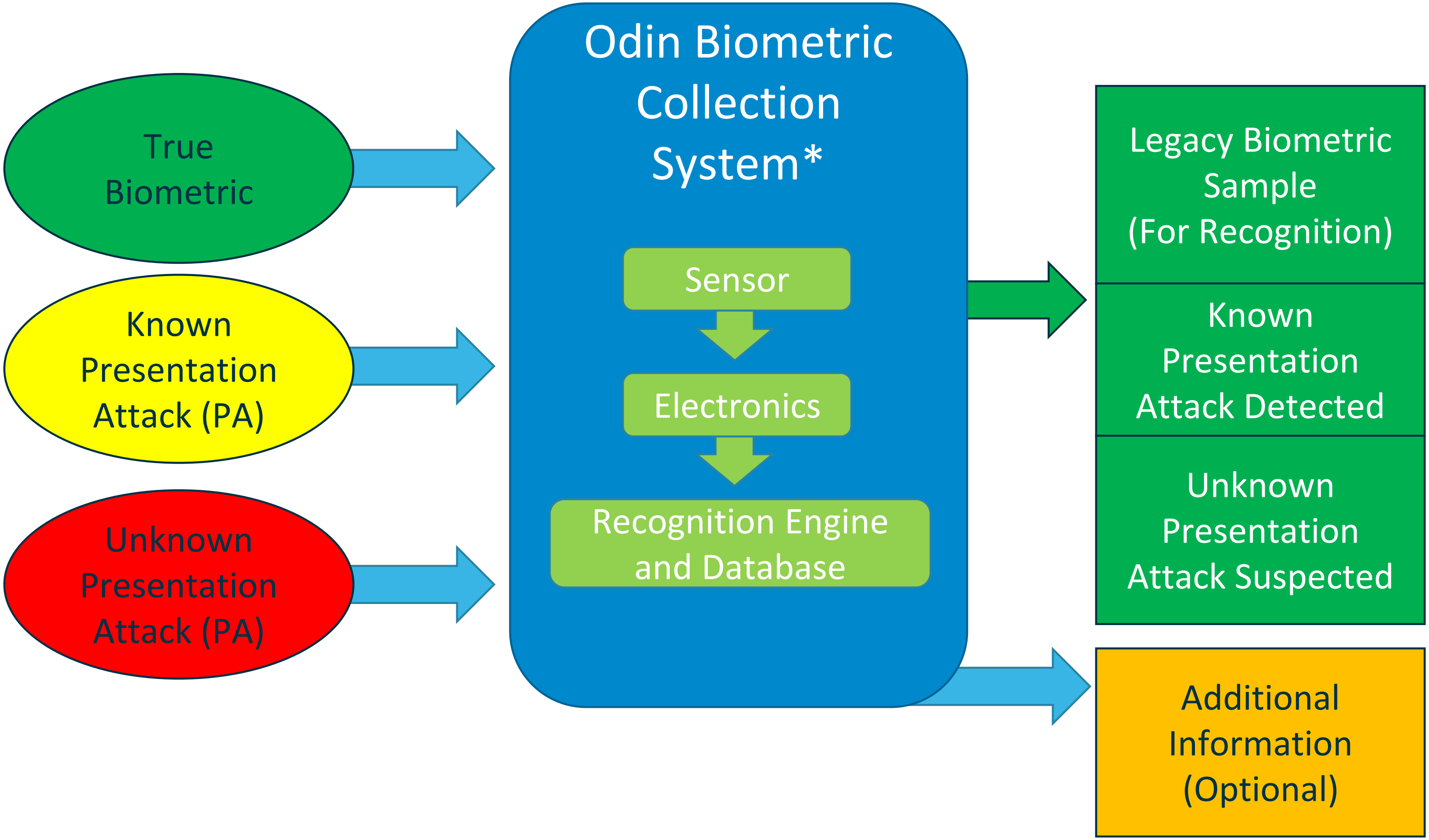
- Capable of detecting known and unknown attacks
- Ability to operate at relevant true/false detection rates
- Biometric recognition at the level of existing technology

Definition of Biometric Presentation Attacks

- Biometric Presentation Attacks (PAs), colloquially referred to as spoofs, are attacks launched against a biometric identification system that intentionally causes the sensor to fail to record the true biometric identity instead recording an alternate identity
  - Traditionally this has been accomplished by a physical prosthetic such as a latex/putty fingerprint







Odin Biometric Collection System*

True Biometric
Known Presentation Attack (PA)
Unknown Presentation Attack (PA)
Sensor
Electronics
Recognition Engine and Database
Legacy Biometric Sample (For Recognition)
Known Presentation Attack Detected
Unknown Presentation Attack Suspected
Additional Information (Optional)

Odin Teams in Phase 2

Phase 2 Teams

Phase 1 Team

Performers

MICHIGAN STATE UNIVERSITY

Clarkson UNIVERSITY

SilkID

PRECISE BIOMETRICS

DELTA ID

CROSSMATCH®
The world identifies with us.℠

FLASHSCAN3D

USC Viterbi School of Engineering

Information Sciences Institute

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

NORTHROP GRUMMAN

idiap RESEARCH INSTITUTE

SRI International®

Compact Imaging

Carnegie Mellon University

Test & Evaluation

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

NIST
National Institute of Standards and Technology

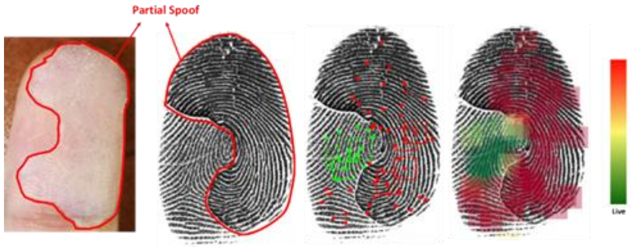
Member of The Family
(Dr. Terry Watters)

Michigan State University

Figures are UNCLASSIFIED

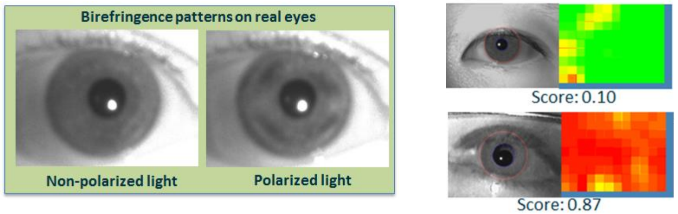
Finger

- **Sensor-based PAD Methods**
  - Open Source FTIR RaspiReader (MSU)
  - Hybrid electro-optic (Silk ID)
  - Fast Frame Rate (Silk ID)
  - Multi-Camera/Multi-Imaging (Silk ID)
- **Image-based PAD Methods**
  - Minutiae-based CNN Approach
  - Dynamic Characteristics of Fingerprint



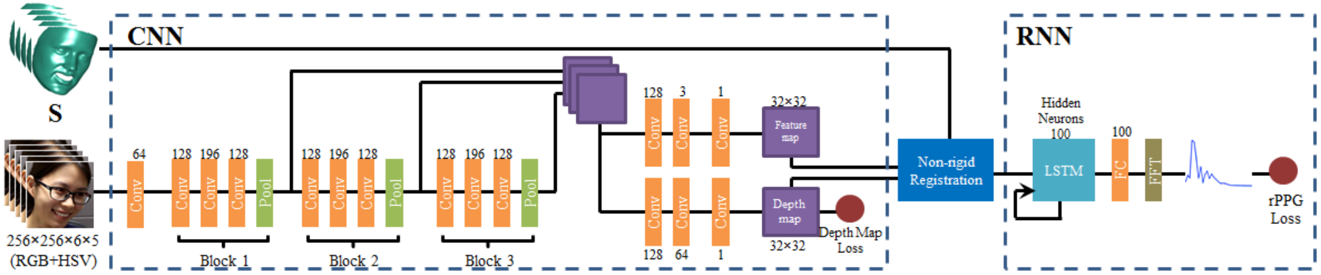
Iris

- **Corneal Birefringence PAD**
  - Human eyes produce birefringence characterized with specific properties
- **Multi-patch CNN**
  - Use deep learning techniques to learn optimal features
  - Examine CNN anatomy to analyze how the models detect PAs



Face

- **CNN Spatial supervision: pseud-depth map estimation**
- **RNN Temporal supervision: rPPG signal estimation**

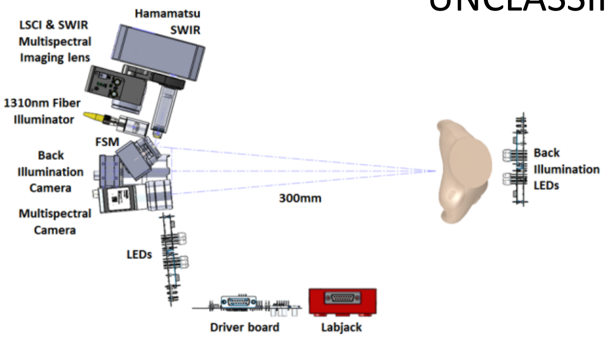


University of Southern California - ISI

Figures are UNCLASSIFIED

Finger

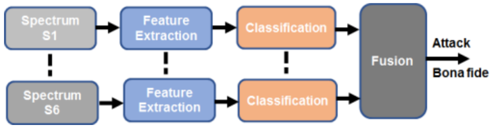
- **Multi-spectral Imaging**
  - CMOS Mono NIR Back-Illumination (940 nm,3072x2048)
  - CMOS Multispectral (Vis/NIR)(same as face)
  - InGaAs Multispectral (SWIR)(same as face)
  - InGaAs Laser Speckle Contrast Imaging (LSCI)(same as face)

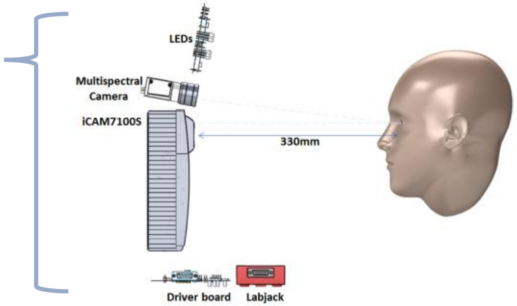


- **Image-based PAD Methods**
  - Luminosity-based PAD
  - Texture-based PAD
  - Blood Motion-based PAD
  - Skin Detection-based PAD

Iris

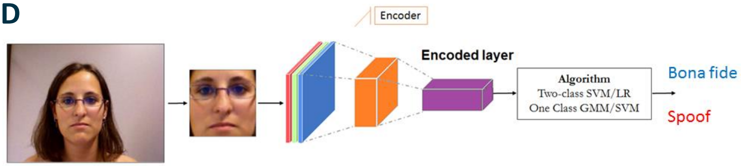
- **Multispectral camera**
  - Visible and 5 near-infrared spectral bands: 800nm, 830nm, 850nm, 870nm and 970nm
- **Software-based PAD**
  - Feature extraction: Gaussian, Laplacian, Steerable pyramids and LBP
  - Classification: SVM, Softmax

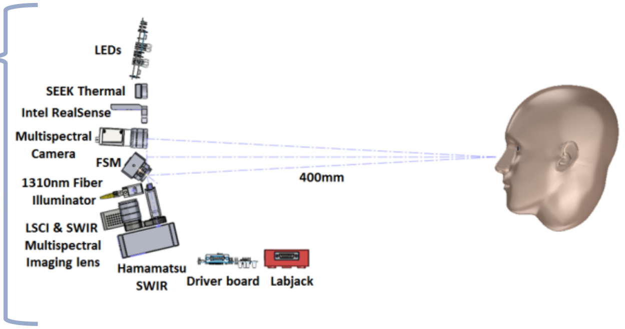




Face

- **Multi-spectral Imaging**
  - Intel RealSense SR300 Camera, Thermal Camera, CMOS Multispectral, Multispectral SWIR, InGaAs Laser Speckle Contrast Imaging (LSCI)
- **Software-based PAD**
  - Motion features caused by facial expression
  - Temporal color changes caused by blood flow





Odin Program Metric

- Presentation Attack Detection
  - **True Detect Rate (TDR) =** Likelihood of correctly identifying a biometric PA
  - **False Alarm Rate(FAR) =** Likelihood of incorrectly identifying a biometric sample as PA when it is a genuine sample
  - **TDR @ FAR < X=** Likelihood of correctly identifying a PA for a fixed likelihood of a false alarm
- Caveat
  - Numbers are not go/no go
  - Meaning is complicated by different PA's

	Phase 1	Phase 2	Phase 3
TDR @ 0.2% FAR	85%	95%	97%
Total Subjects	620	1700	2200

Number of Subjects	90% interval
100	± 8.25%
200	± 5.83%
350	± 4.40%
620	± 3.31%
1,700	± 2.00%
2,200	± 1.76%
5,000	± 1.17%
10,000	± 0.825%
100,000	± 0.26%

Odin Program Constraints

- Biometric Performance
  - **False Match Rate (FMR) =** Likelihood that a system will incorrectly determine that two biometric samples match (e.g., samples belonging to different subjects)
  - **False Non-Match Rate (FNMR) =** Likelihood that a system will incorrectly determine two biometric samples do not match (e.g., samples belonging to the same person)
  - **Determined via baseline testing on the same dataset calibrated on a larger dataset**
- Operational
  - **Projected Component Cost =** total cost of the components of the PAD system at volume (Less than $5,000)
  - **Temporal Representation =** time required to acquire data from subject to determine if biometric sample is a PA (Less than 30 seconds)

Test and Evaluation Objectives

- Phase 1
  - Focus on known PAs
- Phase 2
  - Focus on unknown PAs
- Phase 3
  - Focus on known and unknown PAs while maintaining operational relevance (cost, time, legacy performance)

Phase	Month	Test Type	Attack Trials	True Attempts	Date
1	**9**	**Self**	**50**	**100**	**Dec '18**
1	**13**	**Self**	**60**	**120**	**Apr '18**
1	**14**	**Government**	**200**	**400**	**May '18**
2	26	Self	200	400	Feb '19
2	27	Government	100	200	May '19
2	32	Self	100	400	Aug '19
2	33	Government	200	500	Nov '19
3	38	Self	100	200	Apr '20
3	39	Government	100	250	May '20
3	45	Self	500	750	Nov '20
3	46	Government	500	1000	Dec '21

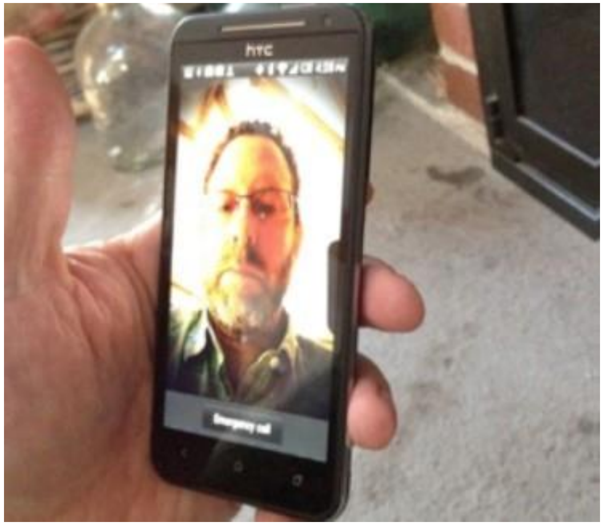
- Government Controlled Tests
  - Goals
    - Collect high quality data that will be used to determine top performers
    - Analyze data results, characterize capabilities
    - Characterize the performance of an array of commercial biometric sensors against a range of presentation attacks

Presentation Attack Recipe Card

Visible Face Video Replay

- **Species:** Face Video Replay
- **Series:** MBGC V1
- **Dependencies:** IRB Defined by IRB governing image collection
  License Approval: MCGC V1 dataset
  Equipment: Computer, tablet or standard monitor
  GFE: N/A
- **Resources**: Expertise: Low
  Lab space: Low
  Storage Space: Low
  Time: Low
  Money: Low
- **Materials**: Computer, tablet or phone display
- **Settings**: Display: Computer, tablet or standard monitor
- **Resolution**: 1920 x 1080
- **Scaling**: 100% (no zoom)
- To download, your institution must sign the license agreement and obtain access to ND Multiple Biometric Grand Challenge v1:https://sites.google.com/a/nd.edu/public-cvrl/data-sets

Graphic is UNCLASSIFIED



ND Multiple Biometric Grand
Challenge (MBGC) V1
Visible Face Video
05186v191.ts
(or similar video)

Odin GCT: Face Presentation Attacks

Figures are UNCLASSIFIED

List of Face Attacks	
Analog photograph Glossy paper	Photo of Drew
Analog photograph Glossy paper	Photo of Diane
Halloween Transparent Mask with Makeup	Old Man Grump
Halloween Transparent Mask with Makeup	Frenchman
High Quality Composite Effects Full Silicone Mask	Mac the Guy
High Quality Composite Effects Full Silicone Mask	Derek
High Quality Composite Effects Full Silicone Mask	Remy the Stranger
Makeup Heavy Contour, COTS makeup	Contour v2
Makeup Old Age, COTS makeup	
Facial Disguise Paper glasses	Peach (light)
Facial Disguise Paper glasses	Brown (dark)
Silicone Partial face mask	Silicone Mask

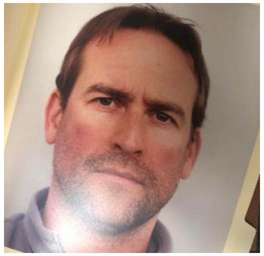
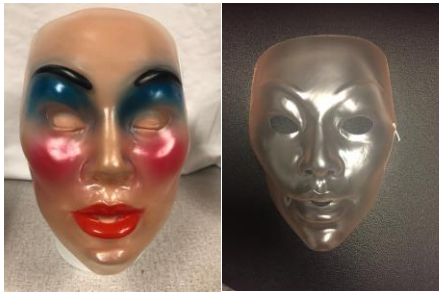


Photo of Drew
Score **1.4**
Complexity **LOW**

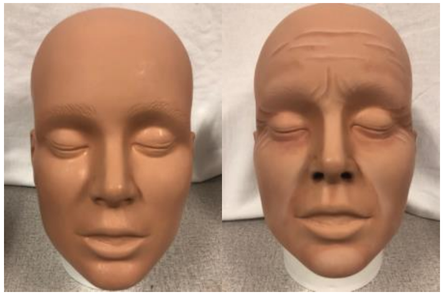
Brown (dark)
Score **1**
Complexity **LOW**

Peach (light)
Score **1**
Complexity **LOW**



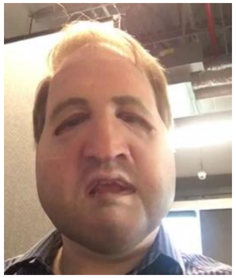
Frenchman with, without Makeup
Score **1**
Complexity **LOW**

Old Man Grump
Score **1**
Complexity **LOW**

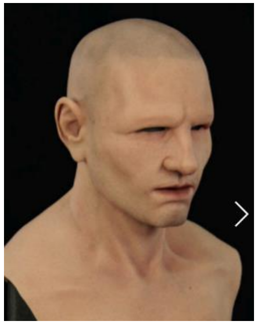


Old Age Makeup
Score **2.5**
Complexity **MEDIUM**

Silicone face mask (Video)



Score **3.6**
Complexity
MEDIUM-HIGH



Mac the Guy

Derek

Remy the Stranger

Score **3.6**
Complexity **MEDIUM-HIGH**

Scale Value	Low	Low-Medium	Medium	Medium-High	High
Coded Value	1	2	3	4	5

Performance on Key Metrics (Phase 1)

H1 (Odin Objective): Harden biometric collection systems against known and unknown presentation attacks (PAs)

- Focus of phase 1 is on detecting known attacks

Finger

	TDR @ 0.2% FAR	AUC
Goal	**85%**	
Baseline	7.0%	0.97
Odin-1	98.6%	1.0
Odin-2	99.1%	1.0
Odin-3	10.4%	0.99
Odin-4	72.9%	0.96

Face

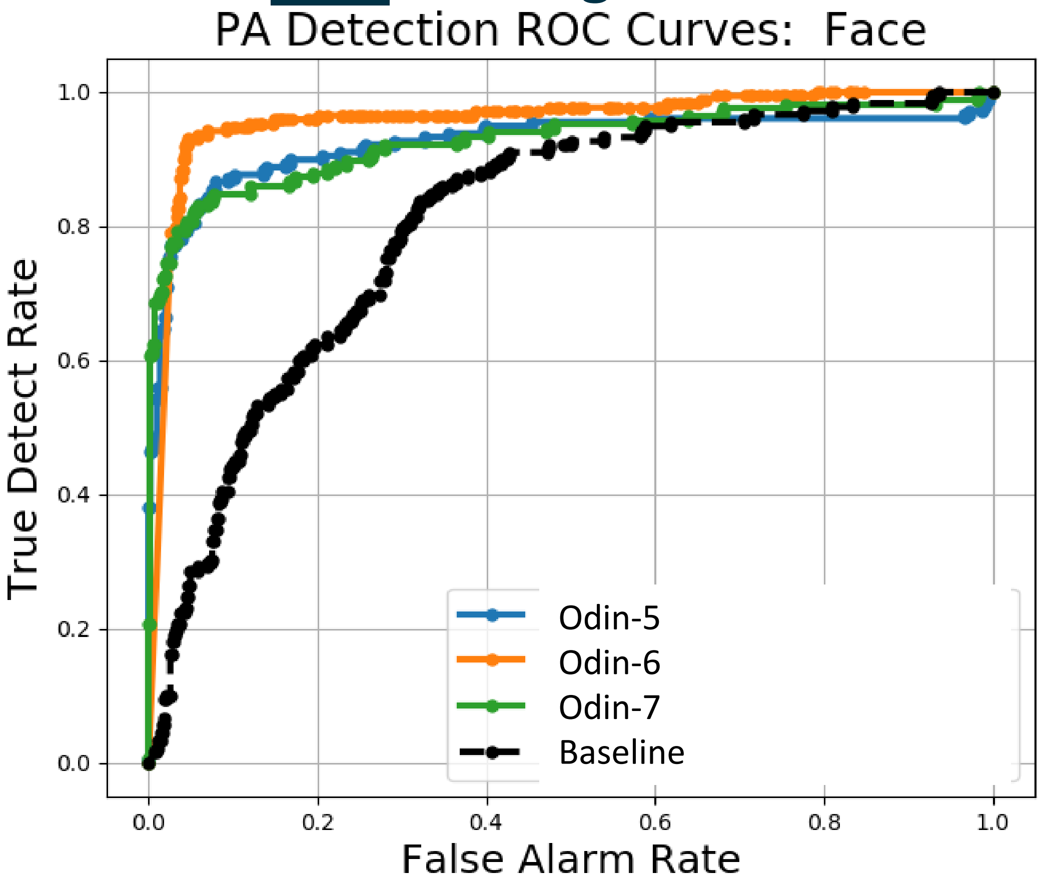
	TDR @ 0.2% FAR	AUC
Goal	**85%**	
Baseline	0.4%	0.81
Odin-5	51.4%	0.93
Odin-6	5.9%	0.96
Odin-7	20.6%	0.93

Iris

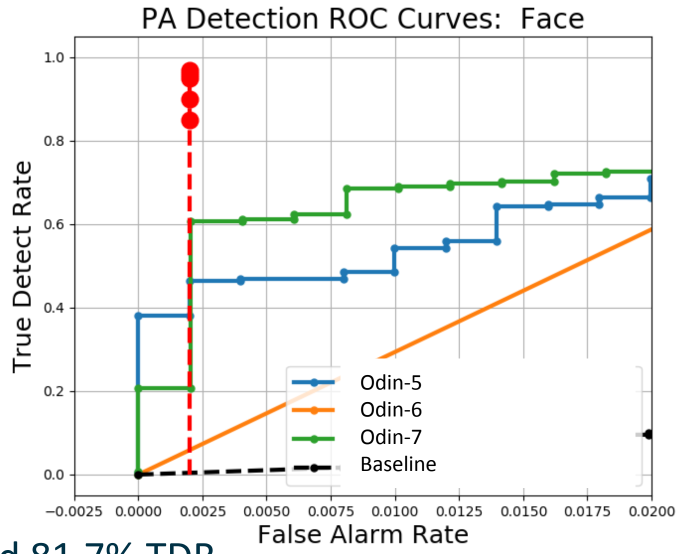
	TDR @ 0.2% FAR	AUC
Goal	**85%**	
Baseline	2.0%	0.8-0.61
Odin-8	71.4%	0.85
Odin-9	39.6%	0.91
Odin-10	4.7%	0.72
Odin-11	0.3%	0.5

Odin GCT-1 Results: Face

Best of Face PAD Algorithms



Algorithm	AUC	TDR @ 0.2% FAR	TDR @ 2% FAR	TDR @ 5% FAR
Odin-5	0.93	51.40%*	70.90%	80.40%
Odin-6	0.96	5.90%	58.80%	93.00%
Odin-7	0.93	20.60%	72.70%	80.60%
Baseline	0.81	0.40%	10.10%	28.70%

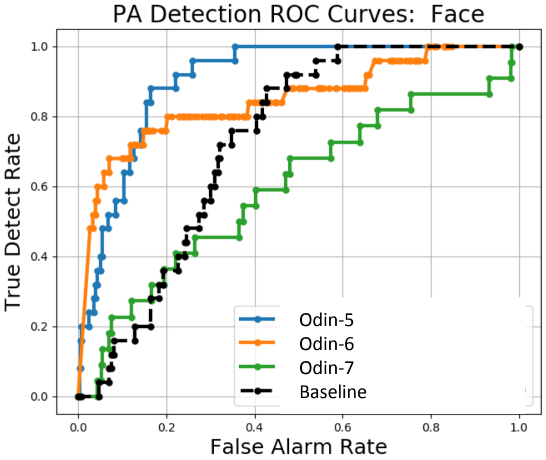


* Errors in submission lowered number, Odin-5 believes they had 81.7% TDR

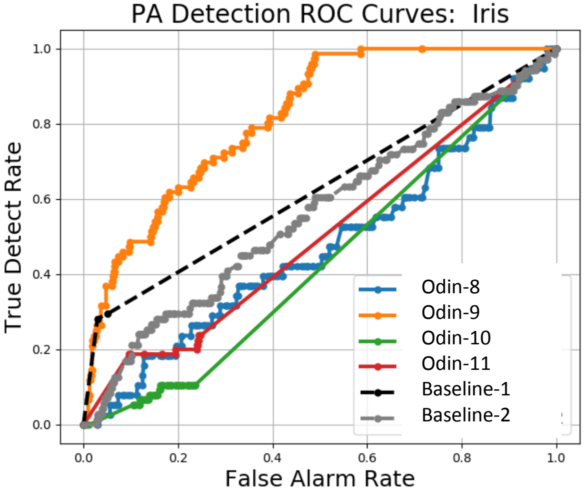
Overall Phase 1 Testing

- Majority of performer approaches beat the baseline PAD solutions on all modalities
- Finger performance was good across all teams and improved significantly beyond baseline methods
- Most performers had trouble with Face and Iris PAD
- Makeup Face PAs most challenging for all performers and baseline
- Contact lens Iris PAs most challenging for all performers and baseline

Face - Makeup



Iris – Contact Lens



Phase 2 Plans

- Focus on detecting unknown PAs
- Two Government Controlled Tests
- Additional emphasis on makeup and contact lenses
- Additional focus on RGB-only solutions for Face

- Prize challenge (tentative Fall 2019)
  - Algorithm PAD challenge
  - Release GCT-2 data with bona fides and PAs from baseline sensors for training/validation
  - In partnership with NIST

Contact Details

Dr. Lars Ericson (Program Manager)

- https://www.iarpa.gov/index.php/research-programs/odin
- Lars.ericson@iarpa.gov
- 301-851-7748

Technical Support

- Dr. Nathan Short
  - Nathan.short@iarpa.gov
  - 301-851-7685
- Dr. Simona Crihalmeanu
  - Simona.crihalmeanu@iarpa.gov
  - 301-699-6438

Programmatic Support

- Ashley Lyles
  - Ashley.lyles@iarpa.gov
  - 301-851-7732

Supplemental Slides

Odin Use Cases

	PA False Alarm Rate	PA True Detect Rate	Cost ($)	Time	Biometric Recognition
Border / Travel Crossing	Small FAR ↓			Fast ↓	Highly Accurate ↑
Visa Applications			Expensive ↑	Long ↑	Highly Accurate ↑
HS Facility Access	Higher FAR ↑	Higher TDR ↑	Expensive ↑	Long ↑	Highly Accurate ↑
HS Cyber Authentication		Higher TDR ↑		Fast ↓	
LS Facility Access					
LS Cyber Authentication		Lower TDR ↓	Cheap ↓	Fast ↓	Low Accuracy ↓

Table is UNCLASSIFED

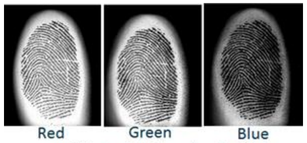
HS = High Security
LS = Low Security

Crossmatch

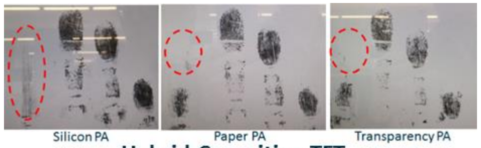
Figures are UNCLASSIFIED

Finger

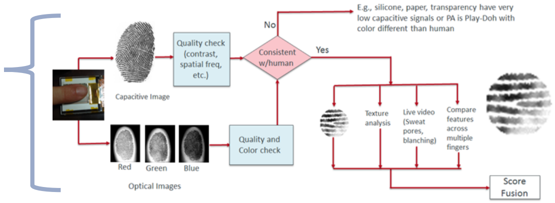
- **Sensor-based PAD Methods**
  - Hybrid TFT Fingerprint Scanner - Scans fingerprints using a contact thin film transistor (TFT) sensor array
  - 3D Structured Light (SLI) Fingerprint Scanner
- **Image-based PAD Methods**
  - Patch-based Deep Learning PAD (Hybrid)
  - Color Analysis (Hybrid)

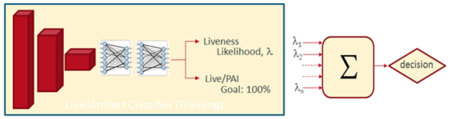


Hybrid Optical TFT



Hybrid Capacitive TFT

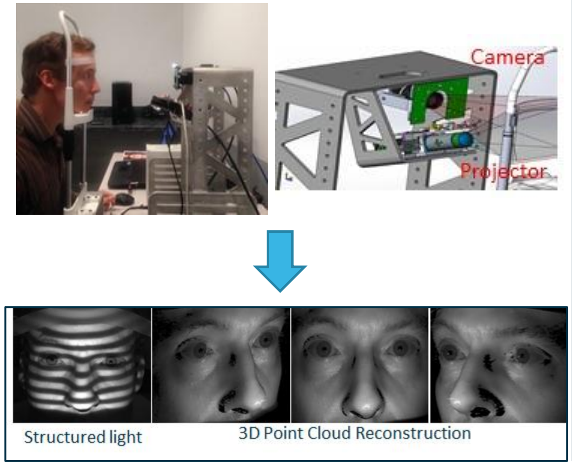

Capacitive Image
Quality check (contrast, spatial freq, etc.)
Consistent w/human
No
Yes
E.g., silicone, paper, transparency have very low capacitive signals or PA is Play-Doh with color different than human
Red
Green
Blue
Optical Images
Quality and Color check
Texture analysis
Live video (Sweat pores, blanching)
Compare features across multiple fingers
Score Fusion

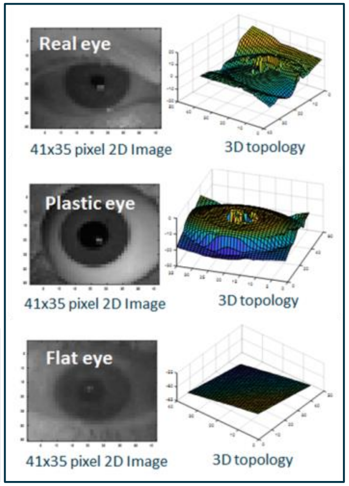


Patch-based Deep Learning

Iris

- **3D Iris Scanner using structured light (SLI)**
  - Device scans both eyes at once; 2D scans with 810 nm LEDs
- **Fusion of 2D and 3D Eye Analysis**
  - 2D Analysis: pupil size vs. iris circularity with polynomial boundary
  - 3D Analysis: investigating large spatial frequency variations
- **Single 2D or 3D CNN PAD; Combined 2D and 3D CNN**
- **Fusion of Iris, Sclera, and Periocular Region Analysis**



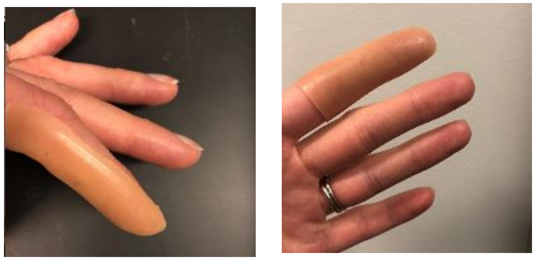


Odin GCT: Fingerprint Presentation Attacks

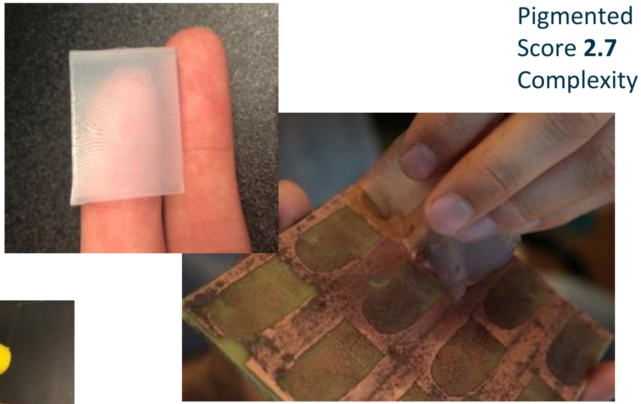
List of Fingerprint Attacks	
Overlay Silicone	Yellow Silicone
Ovelay Silicone + Addition	Fleshtone
Overlay Silicone	Sienna
Overlay Silicone	Nusil - Carbon conductor
Overlay with Conductive silicone (sputter)	Print v2
Overlay PCB Mold with Dragonskin	Print 2 with electrical tape backing
Overlay PCB Mold with Dragonskin modified	Silver Conductive ink, custom design details
Printed fingerprint on glossy paper v1 with conductive ink	
Printed fingerprint on conductive paper v2 (cut modified)	
Printed fingerprint on transparency	

Scale Value	Low	Low-Medium	Medium	Medium-High	High
Coded Value	1	2	3	4	5

Printed fingerprint on Transparency
Score **1**
Complexity **LOW**

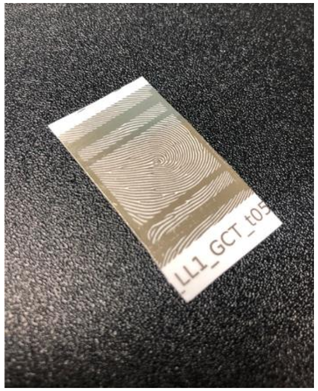


Pigmented Silicone Overlay Fleshtone
Score **2.7**
Complexity **MEDIUM**

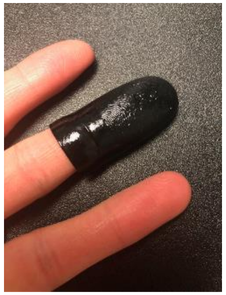


PCM Mold with Dragonskin Overlay
Score **2.3**
Complexity **LOW-MEDIUM**

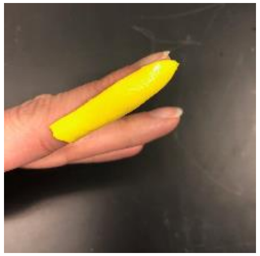
PCM Mold with Dragonskin Modified Overlay
Score **2.5**
Complexity **MEDIUM**



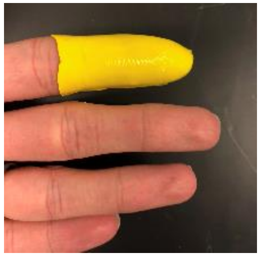
2D printed fingerprint with conductive ink
Score **3.7**
Complexity **MEDIUM-HIGH**



Conductive Silicone Overlay
Score **2.7**
Complexity **MEDIUM**



Yellow Silicone Overlay
Score **2.7**
Complexity **MEDIUM**

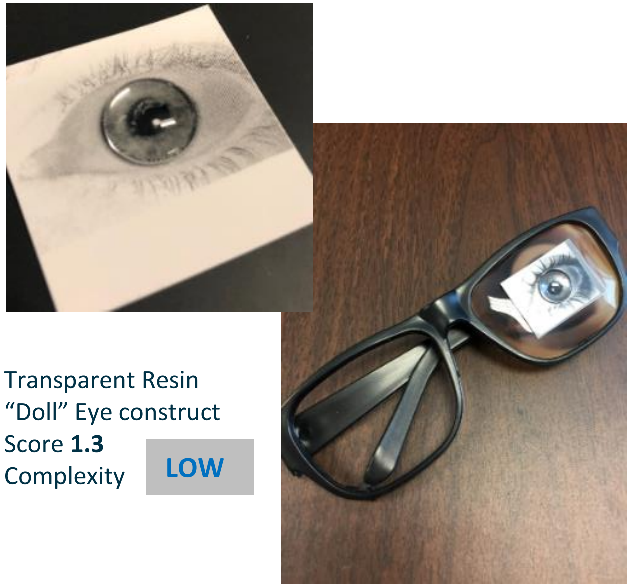


Yellow Silicone Overlay + Addition
Score **3.2**
Complexity **MEDIUM**

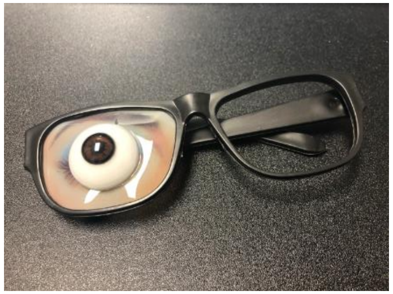
Figures are UNCLASSIFIED

Odin GCT: Iris Presentation Attacks

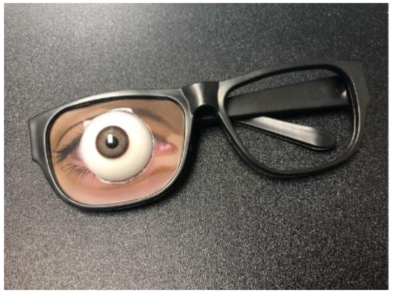
List of Iris Attacks	
Fake Van Dyke eye, mounted	Brown, R
Fake Van Dyke eye, mounted	Hazel, R
Printed iris with molded transparent dome	Transparent resin, Doll eye, R
Cosmetic Contact lens	Acuvue Accent Vivid
Cosmetic Contact lens	Air Optix Blue



Transparent Resin
“Doll” Eye construct
Score **1.3**
Complexity **LOW**



Van Dyke Eye Brown
Score **1.3**
Complexity **LOW**



Van Dyke Eye Hazel
Score 1.3
Complexity **LOW**

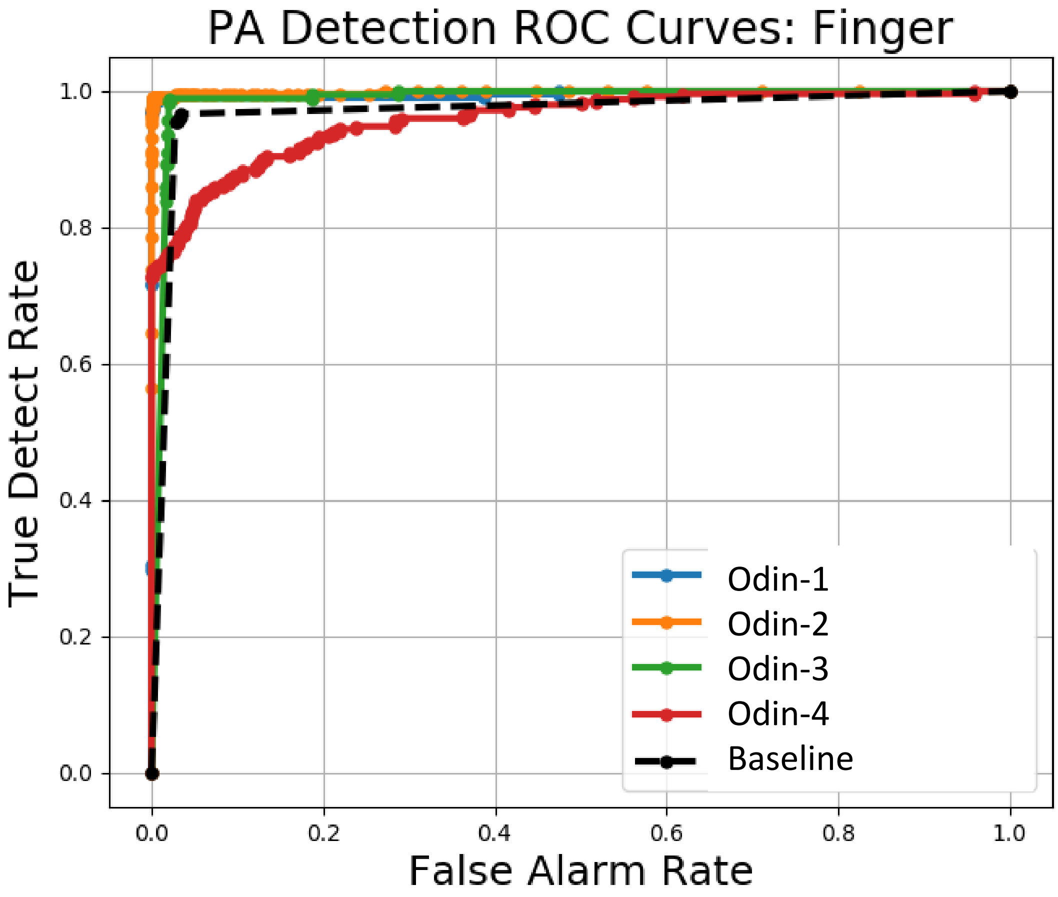
Cosmetic Contact Lens
Score **2.7**
Complexity **MEDIUM**

Scale Value	Low	Low-Medium	Medium	Medium-High	High
Coded Value	1	2	3	4	5

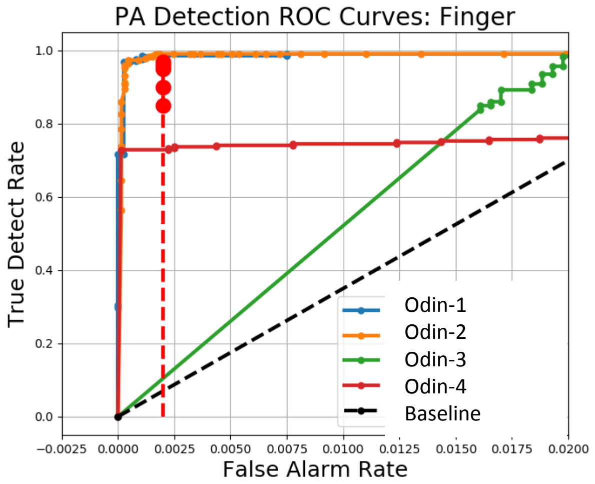
Figures are UNCLASSIFIED

Odin GCT-1 Results: Finger

Best of Finger PAD Algorithms

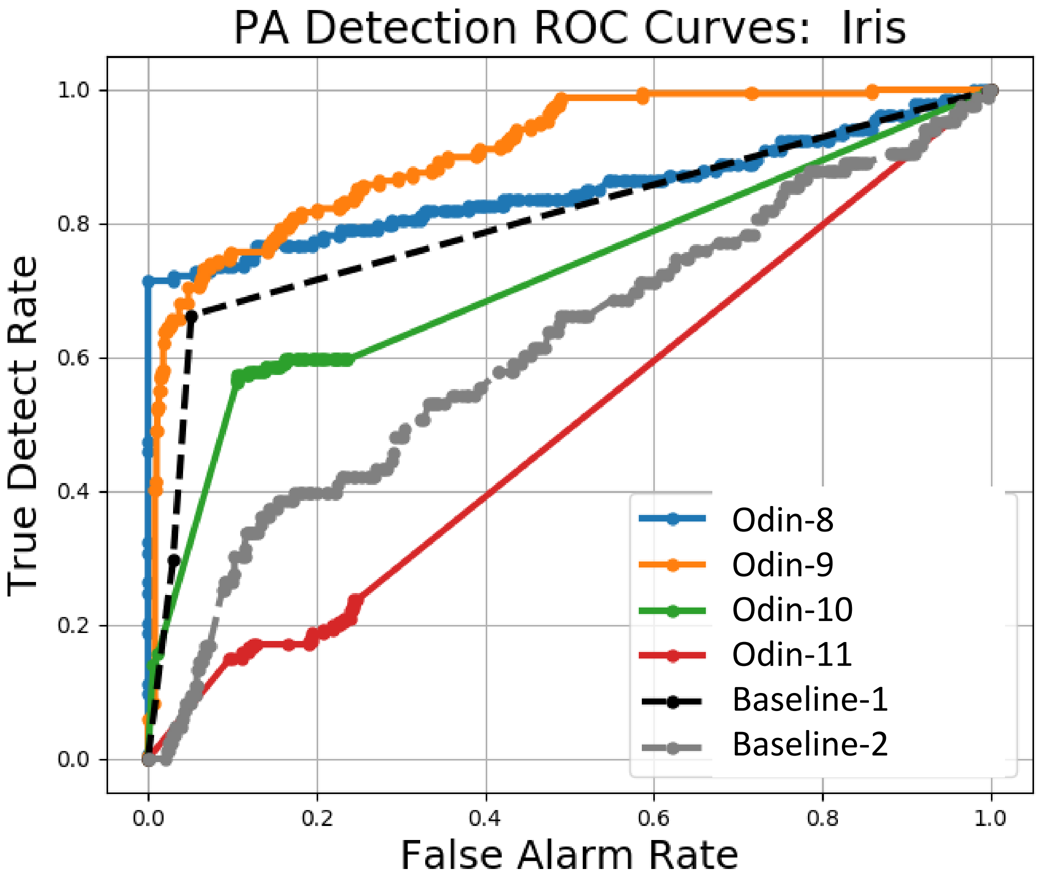


Algorithm	AUC	TDR @ 0.2% FAR	TDR @ 2% FAR	TDR @ 5% FAR
Odin-1	1	98.6%	99.1%	99.1%
Odin-2	1	99.1%	99.1%	99.6%
Odin-3	0.99	10.4%	98.4%	98.9%
Odin-4	0.96	72.9%	76.1%	82.9%
Baseline	0.97	7.0%	7.0%	96.7%

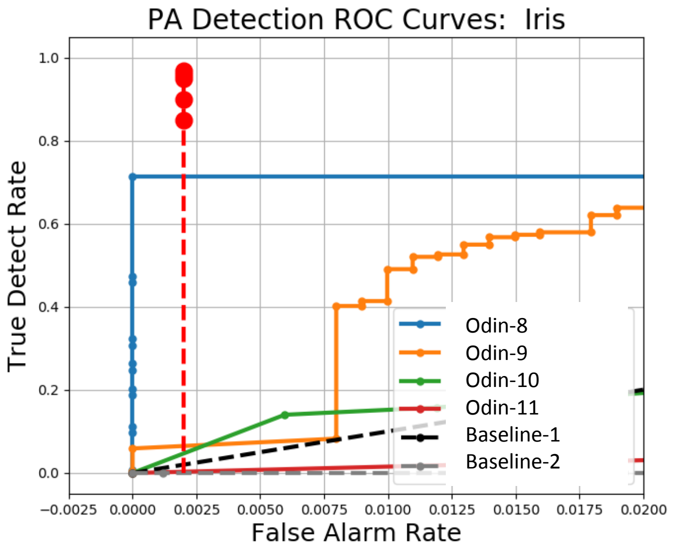


Odin GCT-1 Results: Iris

Best of Iris PAD Algorithms



Algorithm	AUC	TDR @ 0.2% FAR	TDR @ 2% FAR	TDR @ 5% FAR
Odin-8	0.85	71.4%	71.4%	72.2%
Odin-9	0.84	39.6%	55.0%	59.8%
Odin-10	0.72	4.7%	19.3%	32.3%
Odin-11	0.5	0.3%	3.1%	7.7%
Baseline-1	0.8	2.0%	20.1%	64.0%


PA Detection ROC Curves: Iris
True Detect Rate
False Alarm Rate
Odin-8
Odin-9
Odin-10
Odin-11
Baseline-1
Baseline-2